Personally Identifiable Information (PII)

Greater Lincoln Workforce Development Board
03-20-2019

Purpose: This is a board policy to protect personal information relating to an identifiable person

Personally identifiable information (**PII**) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered **PII**.

PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information.

The Greater Lincoln local area must have an internal control structure and written policies in place that provide safeguards to protect personally identifiable information, records, contracts, grant funds, equipment, sensitive information, tangible items, and other information that is readily or easily exchanged in the open market or that is considered to be sensitive, consistent with applicable Federal, State, and local privacy and confidentiality laws.

The Greater Lincoln Workforce Development Board understands the importance of protecting and securing personally identifiable and sensitive information.

Grantee and administrative entity information and practices adhere to the City of Lincoln requirements.

The One Stop Operator and the WIOA Title IB Service Provider are required to have written operational procedures in place in sufficient detail to instruct staff on the importance of protecting personally identifiable information. Any breach of data must be reported in writing to the administrative entity immediately upon occurrence, not to exceed 24 hours after the breach is identified.

Operational procedures in use by the One Stop Operator and Title IB Service Provider must include the elements below:

<u>Participant Data</u>
Participant information shall be stored in a secure location, any electronic transmittal of personal information shall have identifiable information or sensitive information redacted or transmitted in a password-protected document or encrypted. Staff will receive training on procedures for handling sensitive and identifiable personal information and will be required to sign a confidentiality agreement as a condition of employment, to be kept on file.

This process is shared with participants through a Consent/Authorization Form. Each participant is required to verify they have been informed about this process by signing the form.

<u>One Stop Operator/Title IB Provider Employee Data</u>
The One Stop Operator/IB Provider will take reasonable technical and organizational precautions to prevent the loss, misuse or alteration of personal information and intellectual property. The Operator/Provider will store all personal information provided in a secure location.